35. Encoding of Linear Block Codes

Consider the coded digital communication system model shown in Figure 35.1.

Figure 35.1 Model of a coded digital communication system.

A sequence of q-ary digits called the information vector $\mathbf{U} = [u_0\ u_1\ ...\ u_{k-1}]$ is fed into a block encoder. The block encoder adds redundancy digits to **U** and produces an encoded vector $\mathbf{V} = [v_0\ v_1\ ...\ v_{n-1}]$ called a channel codeword. A set of q^k q-ary vectors (codewords) of length n defines a block code. In most applications, $q = 2$ and the block code is binary in nature. The modulator transforms the encoded vector into a modulated signal vector which is suitable for transmission through the analog channel. At the receiving end, the demodulator performs an inverse operation and produces a received vector $\mathbf{R} = [r_0\ r_1\ ...\ r_{n-1}]$. Subject to noise disturbance, the received vector **R** may not be the same as the encoded vector **V**. The channel decoder uses the redundancy in the encoded vector **V** to correct the errors in the received vector **R** and produces an estimated of **U**, denoted as $\hat{\mathbf{U}} = [\hat{1}_0\ \hat{1}_1\ ...\ \hat{1}_{k-1}]$.

Basic Concepts and Definitions

Consider the following examples where k number of information digits are fed into a channel encoder and n number of encoded digits are produced by the channel encoder. This is shown in Figure 35.2.

Figure 35.2 Block diagram for a block encoder.

Example 35.1

Suppose $q = 2$, $k = 3$ and $n = 3$. The codewords are {0 0 0, 0 0 1, 0 1 0, 0 1 1, 1 0 0, 1 0 1, 1 1 0, 1 1 1}. Clearly, the codewords contain no redundancy if $k = n$. A single error will carry one transmitted codeword into another codeword, and the error will not be detected.

Example 35.2

Suppose $q = 2$, $k = 2$ and $n = 3$. There are $2^k = 4$ possible input patterns and $2^n = 8$ possible output patterns. A possible encoding rule is shown in Table 35.1.

Table 35.1
Mapping Rule for the Block Encoder in Example 35.2

Information Vector **U**	*Codeword* **V**
0 0	0 0 0
0 1	0 1 1
1 0	1 0 1 } 2 bits in difference
1 1	1 1 0

If 1 0 1 is transmitted, an error pattern **E** = [0 0 1] will convert 1 0 1 to 1 0 0, the received vector **R**. If the channel decoder has a complete knowledge of Table 35.1 and chooses the output pattern corresponding to the minimum number in bit differences from the received vector **R** as the estimated information vector $\hat{\mathbf{U}}$, the decoder cannot decide whether 0 0 0, 1 0 1 or 1 1 0 is the estimate of the information vector **U**. This is because 0 0 0, 1 0 1 and 1 1 0 differ in one place from the received vector **R** = [1 0 0]. However, an error is detected. To complete the decoding process, a codeword is chosen by a random selection process and the decoder commits a decoding error.

Example 35.3

Suppose $q = 2$, $k = 1$ and $n = 3$. There are $2^k = 2$ possible input patterns and $2^n = 8$ possible output patterns. A possible encoding rule is shown in Table 35.2.

Table 35.2
Mapping Rule for the Block Encoder in Example 35.3

Information Vector **U**	*Codeword* **V**
0	0 0 0 } 3 bits in difference
1	1 1 1

If 0 0 0 is transmitted, an error pattern **E** = [0 0 1] will convert 0 0 0 to 0 0 1, the received vector **R**. If the channel decoder has a complete knowledge of Table 35.2 and chooses the output pattern corresponding to the minimum number in bit differences from

the received vector **R** as the estimated information vector $\hat{\mathbf{U}}$, the decoder will pick 0 0 0 as the estimate of **U**. This is because the received vector **R** = [0 0 1] is closer to the output pattern 0 0 0 than the output pattern 1 1 1. In the presence of a single error, the error is detected and corrected.

In general, there are three problems which face the designer of error detection/correction systems.

1. To synthesis a code with the desired redundancy properties; and hence, to design the encoder;

2. To find a reasonably simple decoder;

3. To make the overall coding system as efficient as possible, so that the minimum amount of redundant information is transmitted.

Definition 35.1. The *Hamming weight* of a vector is defined as the number of nonzero elements contained in the vector.

Definition 35.2. The *Hamming distance* $d(\mathbf{X}, \mathbf{Y})$ between two vectors **X** and **Y** of length n is the number of places in which their elements differ.

Definition 35.3. A block code of size q^k with q symbols is a set or a collection of q^k q-ary vectors (codewords) of length n.

Definition 35.4. The *minimum (Hamming) distance* $d_{\min}$ of a code is the smallest Hamming distance between distinct codewords.

Definition 35.5. A code of length n, with k information digits, is described as an (n, k) code, and if the code has a minimum Hamming distance $d_{\min}$, we describe the code as an (n, k, $d_{\min}$) code. The *dimension* of the code is k.

Definition 35.6. The *rate* of the code R_C is the number of information digits in each codeword divided by the length of the code.

$$R_C = k/n. \tag{35.2}$$

Definition 35.7. A block code of length n and q^k codewords is called a (n, k) q-ary linear code if and only if its q^k codewords form a k-dimensional subspace of the vector space of all n-tuples over the $GF(q)$.

Matrix Description of Linear Block Codes

From Definition 35.7, it is possible to find k linearly independent codewords $\mathbf{G}_0$, $\mathbf{G}_1$, ..., $\mathbf{G}_{k-1}$ in the q-ary code C such that

$$\mathbf{V} = u_0 \mathbf{G}_0 + u_1 \mathbf{G}_1 + ... + u_{k-1} \mathbf{G}_{k-1}, \tag{35.3}$$

where

$$\mathbf{V} = [v_0 \; v_1 \; ... \; v_{n-1}]. \tag{35.4}$$

u_i and v_j are q-ary symbols for $0 \leq i \leq k-1$ and $0 \leq j \leq n-1$. $\mathbf{V}$ is a linear combination of the k linearly independent codewords. The k-by-n *generator matrix* $\mathbf{G}$ of the code C is

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ \vdots \\ \mathbf{G}_{\mathbf{k}-1} \end{bmatrix} \tag{35.5}$$

$$= \begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix} \tag{35.6}$$

where $\mathbf{G}_i = [g_{i,0} \; g_{i,1} \; ... \; g_{i,n-1}]$ with q-ary entries for $0 \leq i \leq k-1$. The encoding operation, as shown in Figure 35.2, can be expressed as

$$\mathbf{V} = \mathbf{U} \; \mathbf{G} \tag{35.7}$$

where

$$\mathbf{U} = [u_0 \; u_1 \; ... \; u_{k-1}] \tag{35.8}$$

Example 35.4

Consider a (7, 4) binary linear block code with $\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$. The information and code vectors are shown as below.

U	**V**
0 0 0 0	0 0 0 0 0 0 0
0 0 0 1	0 0 0 1 0 1 1
0 0 1 0	0 0 1 0 1 1 0
0 0 1 1	0 0 1 1 1 0 1
0 1 0 0	0 1 0 0 1 1 1
0 1 0 1	0 1 0 1 1 0 0
0 1 1 0	0 1 1 0 0 0 1
0 1 1 1	0 1 1 1 0 1 0
1 0 0 0	1 0 0 0 1 0 1
1 0 0 1	1 0 0 1 1 1 0
1 0 1 0	1 0 1 0 0 1 1
1 0 1 1	1 0 1 1 0 0 0
1 1 0 0	1 1 0 0 0 1 0
1 1 0 1	1 1 0 1 0 0 1
1 1 1 0	1 1 1 0 1 0 0
1 1 1 1	1 1 1 1 1 1 1

There exists an (n-k)-by-n matrix **H** with n-k linearly independent rows such that

$$\mathbf{G}\ \mathbf{H}^T = \mathbf{0} \tag{35.9}$$

$$\mathbf{U}\ \mathbf{G}\ \mathbf{H}^T = \mathbf{0}$$

$$\mathbf{V}\ \mathbf{H}^T = \mathbf{0} \tag{35.10}$$

where $\mathbf{H}^T$ is the transpose of the matrix **H**. It follows that any codeword **V** in C generated by **G** is orthogonal to every row of **H**. Therefore, **H** is the *parity-check matrix* of the linear code C. **H** can therefore be thought of as the generator of the *dual code* to that generated by **G**.

The (n - k)-by-n parity-check matrix **H** takes the following form :

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_0 \\ \mathbf{H}_1 \\ \vdots \\ \mathbf{H}_{\mathbf{n}-\mathbf{k}-1} \end{bmatrix} \tag{35.11}$$

$$= \begin{bmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,n-1} \\ \vdots & \vdots & & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{bmatrix} \tag{35.12}$$

where $\mathbf{H}_i = [h_{i,0}\ h_{i,1}\ \ldots\ h_{i,n-1}]$ with q-ary entries for $0 \le i \le n$-k-1. Given the generator matrix **G** of an (n, k) linear code, we can put the generator matrix **G** into systematic form $\mathbf{G}_{\text{SEF}}$ by row/column transformations.

Example 35.5

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ \mathbf{G}_2 \\ \mathbf{G}_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$\mathbf{G}_{\text{SEF}} = \begin{bmatrix} \mathbf{G}'_0 \\ \mathbf{G}'_1 \\ \mathbf{G}'_2 \\ \mathbf{G}'_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

where $\mathbf{G}'_0 := \mathbf{G}_0 + \mathbf{G}_2 + \mathbf{G}_3$, $\mathbf{G}'_1 := \mathbf{G}_1 + \mathbf{G}_3$, $\mathbf{G}'_2 := \mathbf{G}_2$, and $\mathbf{G}'_3 := \mathbf{G}_3$.

When an (n, k) code is generated by the generator matrix $\mathbf{G}_{\text{SEF}}$, the code is called a *systematic code*. The format of a codeword can take the following form as shown in Figure 35.3.

Figure 35.3 Code vector generated by a systematic block code.

The generator matrix for an (n, k) systematic linear code is

$$\mathbf{G}_{\text{SEF}} = \begin{bmatrix} 1 & 0 & \cdots & 0 & p_{0,0} & p_{0,1} & \cdots & p_{0,n-k-1} \\ 0 & 1 & \cdots & 0 & p_{1,0} & p_{1,1} & \cdots & p_{1,n-k-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} \end{bmatrix} \quad (35.13)$$

and the parity-check matrix $\mathbf{H}_{\text{SEF}}$ is

$$\mathbf{H}_{\text{SEF}} = \begin{bmatrix} -p_{0,0} & -p_{1,0} & \cdots & -p_{k-1,0} & 1 & 0 & \cdots & 0 \\ -p_{0,1} & -p_{1,1} & \cdots & -p_{k-1,1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ -p_{0,n-k-1} & -p_{1,n-k-1} & \cdots & -p_{k-1,n-k-1} & 0 & 0 & \cdots & 1 \end{bmatrix} \quad (35.14)$$

For binary linear codes, $-p_{i,j} = p_{i,j}$ for $0 \le i \le k - 1$ and $0 \le j \le n - k - 1$.

Relationship of Minimum Distance to Error Detection and Correction

From Definition 35.4, the minimum Hamming distance of a code is the smallest Hamming distance between distinct codewords. For a linear block code, the all-zero vector is a codeword. Clearly, the minimum Hamming distance is equal to the *minimum weight* of its nonzero codeword, denoted as $w_{\min}\{\mathbf{V}\}$.

Given the parity-check matrix **H** of an (n, k) linear code, one can determine the minimum distance of the code using the following theorem.

Theorem 35.1. For an (n, k) linear block code, the minimum weight of a linear code is equal to the smallest number of columns of **H** that sums to zero.

Proof. $\mathbf{V}\ \mathbf{H}^T = v_0[h_{0,0}\ h_{1,0}\ \ldots\ h_{n-k-1,0}] + v_1[h_{0,1}\ h_{1,1}\ \ldots\ h_{n-k-1,1}] + \ldots + v_{n-1}\ [h_{0,n-1}\ h_{1,n-1}\ \ldots\ h_{n-k-1,n-1}] = \mathbf{0}$. The code symbol v_j is associated with the vector $[h_{0,j}\ h_{1,j}\ \ldots\ h_{n-k-1,j}]$, for $0 \le j \le n-1$, and $[h_{0,j}\ h_{1,j}\ \ldots\ h_{n-k-1,j}]$ corresponds to the j-th column of **H**. Since the minimum Hamming distance of a linear block code is equal to the minimum weight of its nonzero codeword. Clearly, the minimum weight of a linear block code is equal to the smallest number of columns of **H** that sums to zero. □

The parameter d_{min} can be used to predict the error protection capability of a code. A code can correct t' errors, where t' is upper bounded by $(d_{min} - 1)/2$, i.e.,

$$t' = \lfloor (d_{min} - 1) / 2 \rfloor \quad (35.15)$$

or

$$t' \leq (d_{min} - 1) / 2 \quad (35.16)$$

Here $\lfloor (d_{min} - 1) / 2 \rfloor$ denotes the greatest integer less than or equal to $(d_{min} - 1) / 2$. The error-correcting capability of a code is best understood by visualising codewords and arbitrary words as points in geometric space. Each codeword is placed in the center of a sphere of radius t'. These spheres are all disjointed. Words that have t' or fewer errors from a codeword will lie in the respective sphere and closer to that codeword. Since the minimum separation between centers of pairs of sphere is equal to the minimum distance of the code, t' errors can be correctly decoded as long as $2t' + 1 \leq d_{min}$. This is shown in Figure 35.4.

Figure 35.4 A code with minimum Hamming distance $2t' + 1$.

In general, a code can correct any combination of t' errors and detect up to e errors ($e \geq t'$) if

$$e + t' \leq d_{min} - 1 \quad (35.17)$$

Figure 35.5 illustrates the geometric situation. Again, each codeword is placed in the center of a sphere of radius t'. The spheres are all disjointed. Words that have t' or fewer errors from a codeword will lie inside the respective sphere, and the errors can be corrected. If the number of errors are greater than t' but less than e, words will lie outside all these spheres and errors are detected but not corrected.

Figure 35.5 A code with minimum Hamming distance $t' + e + 1$.

Depending on the requirements of the application, a decoder can be designed to detect errors only, correct errors only, or a combination of error detection and error correction. Given the minimum Hamming distance of a code, Table 35.3 gives some possible decoding choices to detect errors and correct errors.

Table 35.3
Some Possible Decoding Choices to Detect Errors and Correct Errors

$d_{\min}$	1	2	3	4	5
e	0	1	2 1	3 2	4 3 2
t'	0	0	0 1	0 1	0 1 2

Given the values of n and k, what is the minimum Hamming distance of an (n, k) linear code. The following theorem provides an upper bound to the minimum distance of an (n, k) linear code

Theorem 35.2. (Singleton bound) The minimum distance of an (n, k) linear code is

$$d_{\min} \le n - k + 1 \tag{35.19}$$

Proof. The maximum number of linearly independent column vectors in the parity-check matrix **H** is $(n - k)$. A codeword with only one non-zero information symbol cannot have weight larger than $n - k + 1$. Therefore, $d_{\min} \le n - k + 1$. □

Reference

Lee, L. H. C., Error-Control Block Codes for Communications Engineers, Artech House, 2000.

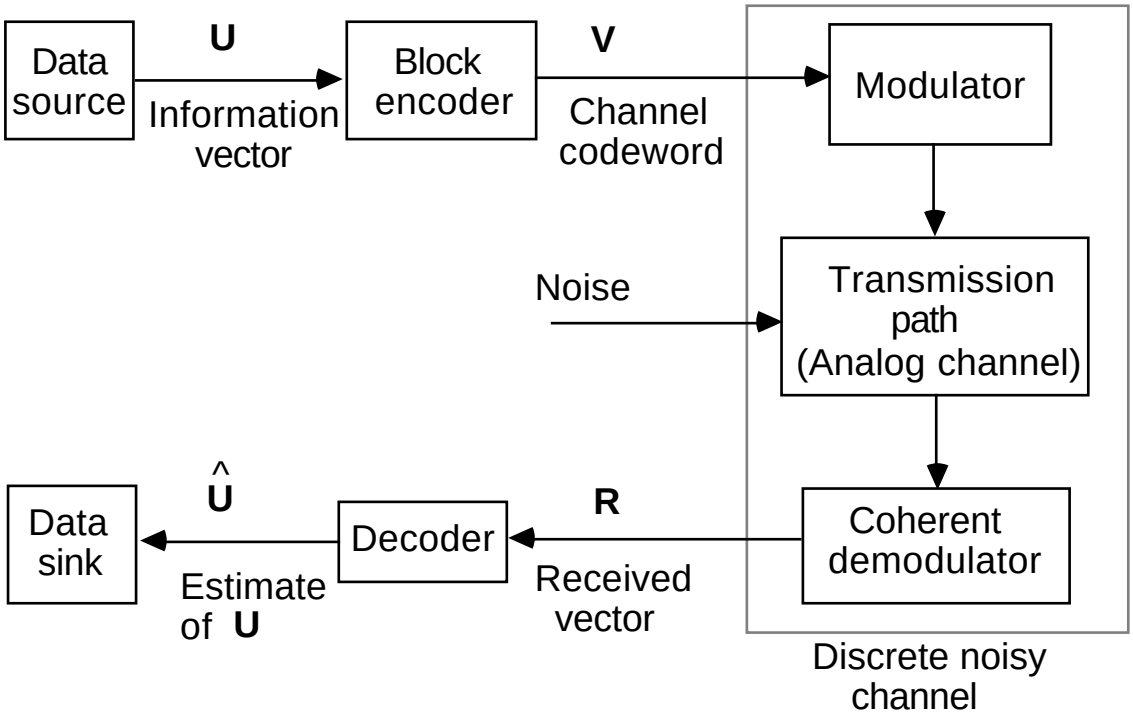

Figure 35.1 Model of a coded digital communication system.

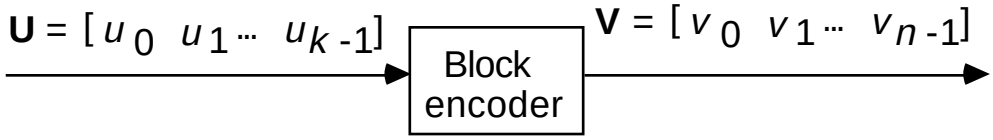

Figure 35.2 Block diagram for a block encoder.

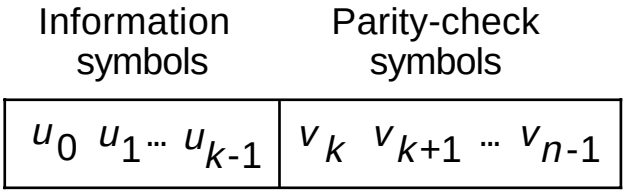

Figure 35.3 Code vector generated by a systematic block code.

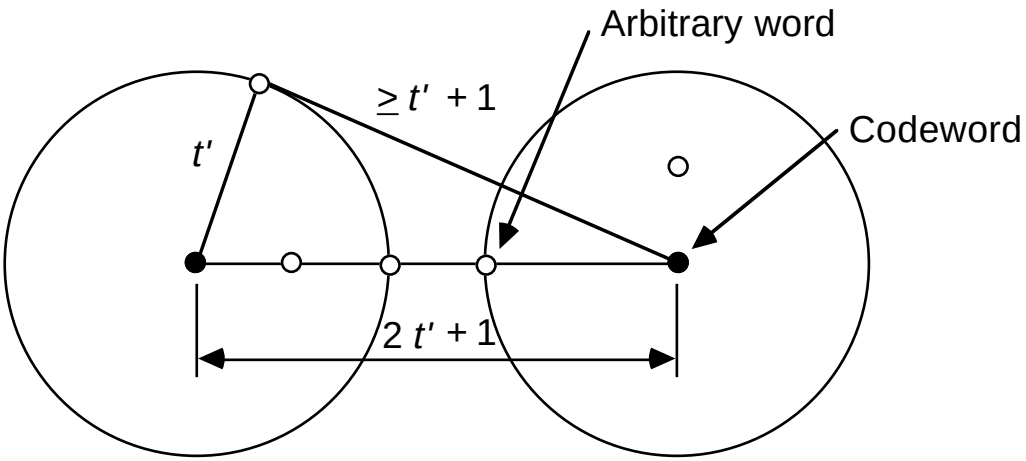

Figure 35.4 A code with minimum Hamming distance 2*t*' + 1.

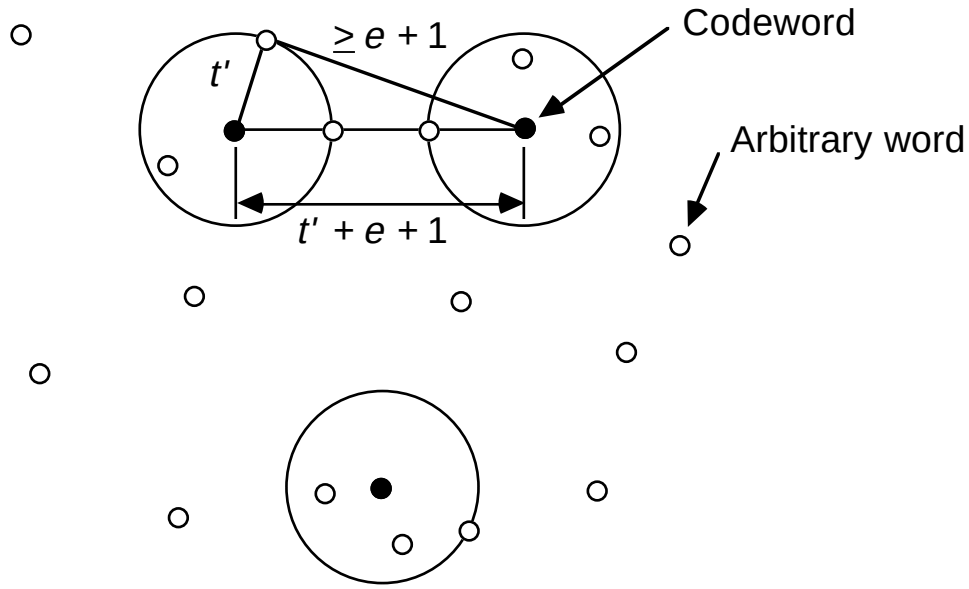

Figure 35.5 A code with minimum Hamming distance *t*' + *e* + 1.